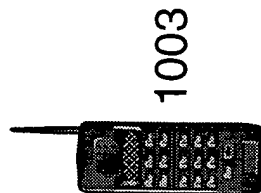
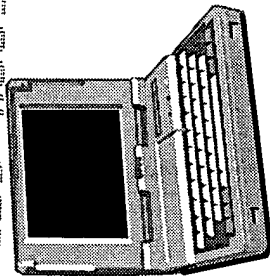


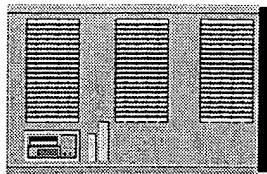
661250-40897E60



1003



1001



1005

Inquiry 1010

Inquiry Result, Identifier 1020

1015

Enter PIN 1025

Establish Secure Connection 1030

1035 Generate Public/Private Key Pair 1050

1045 Create Certificate 1015 1040

1055 Establish Secure Connection

1060 Send Certificate

1050

A65 Sign Certificate

Send Signed Certificate

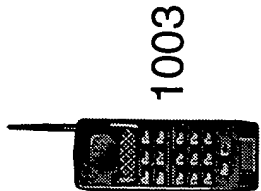
1070

1050'

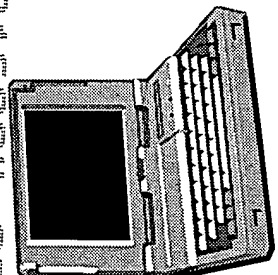
Store Signed Certificate 1075

Fig. 1A

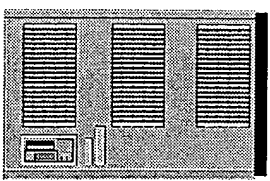
661250"4089760



1003



1001



1005

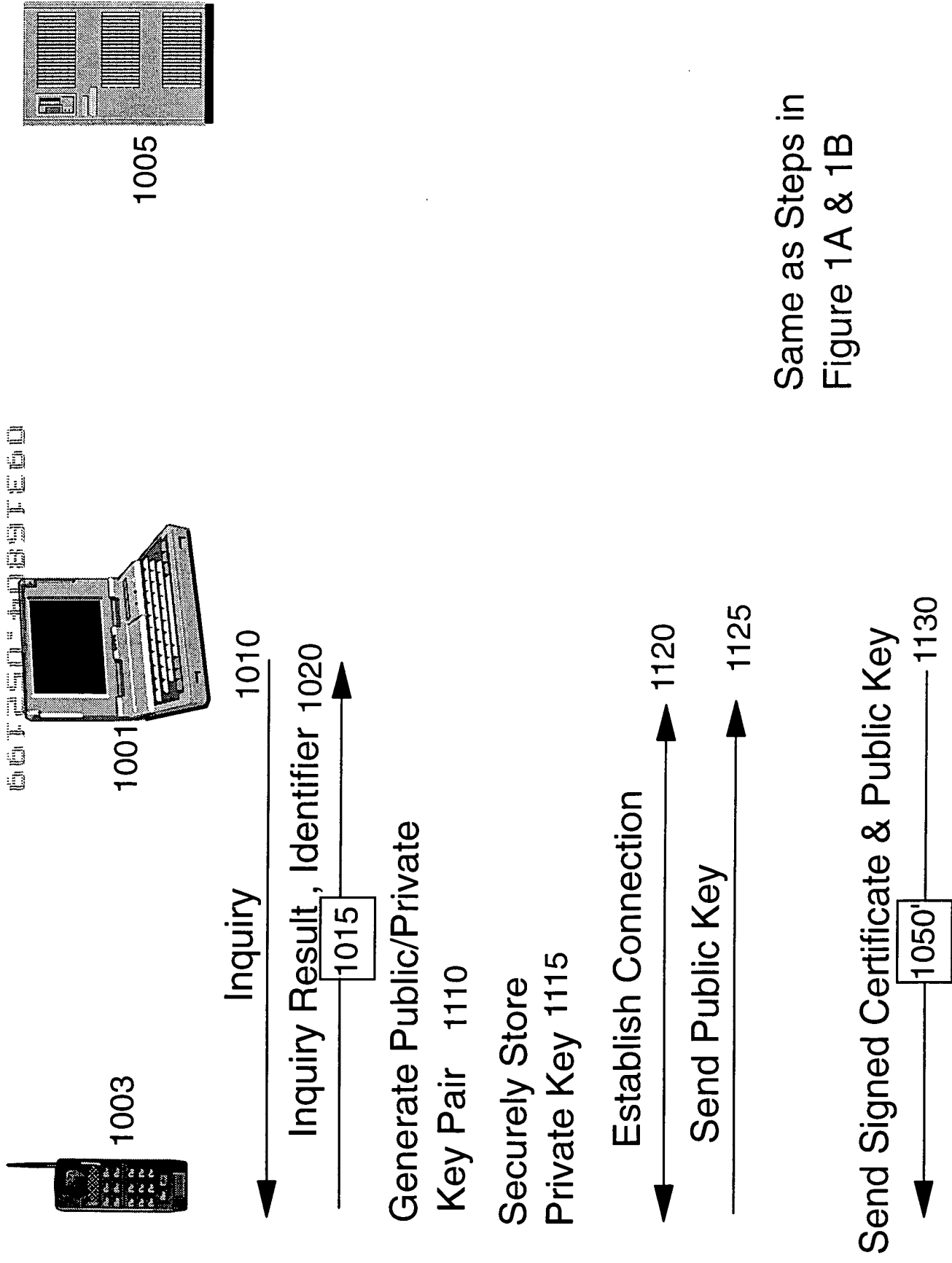
1080 Send Cert. & Keys, Disconnect

Store Signed Certificate
and Public Key 1085

Store Private Key 1090
as Protected Value

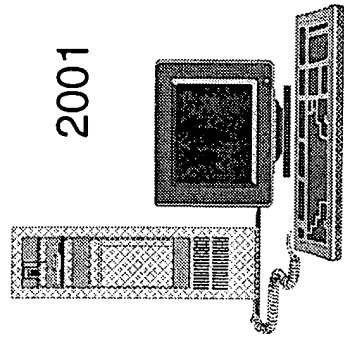
| | | |
|------------|------|------------|
| Delete PIN | 1095 | Delete PIN |
|------------|------|------------|

Fig. 1B

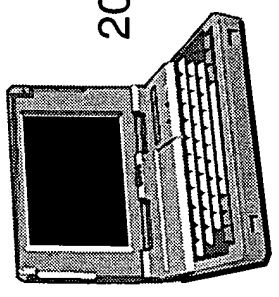


Same as Steps in
Figure 1A & 1B

Fig. 1C



2001



2003

Authentication

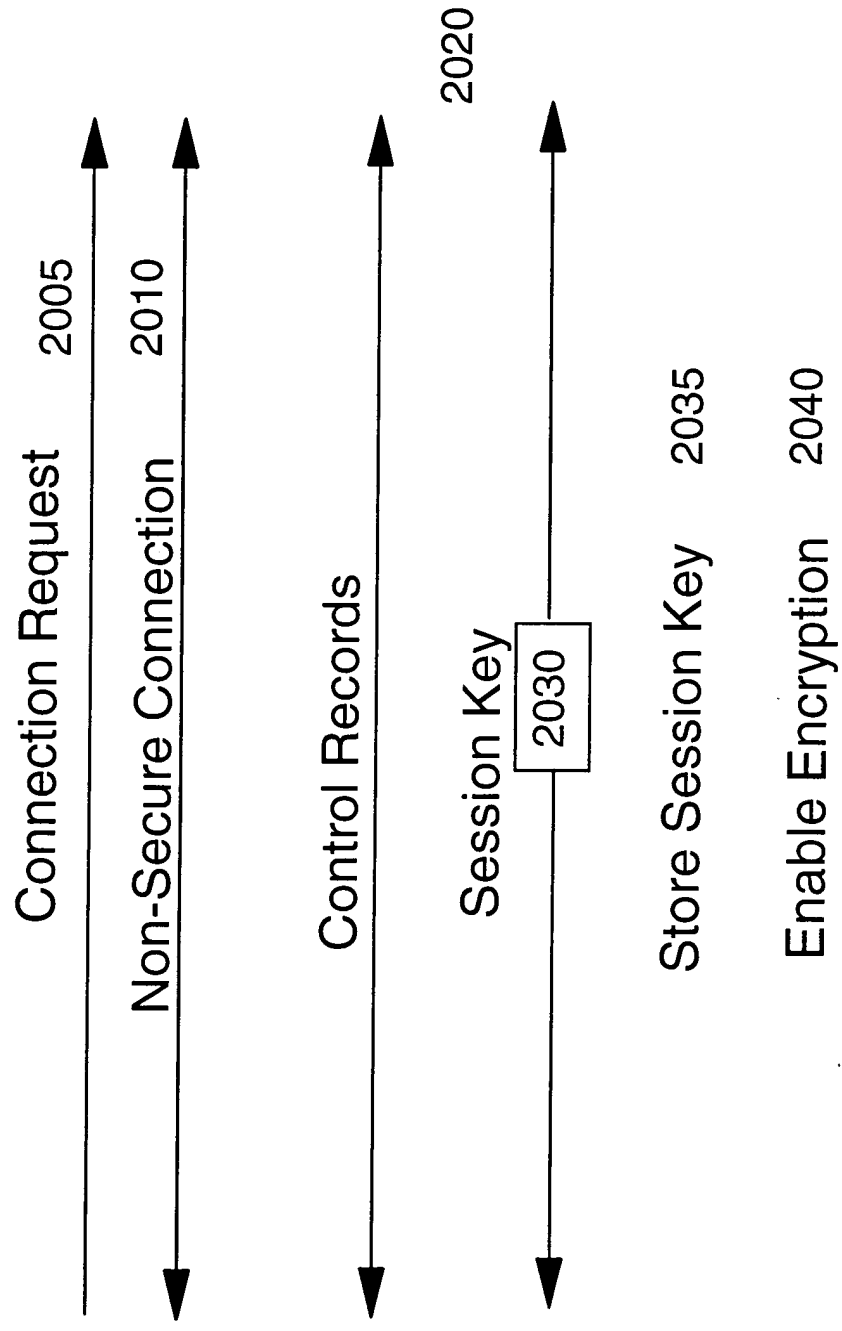


Fig. 2

661250-1089TE60

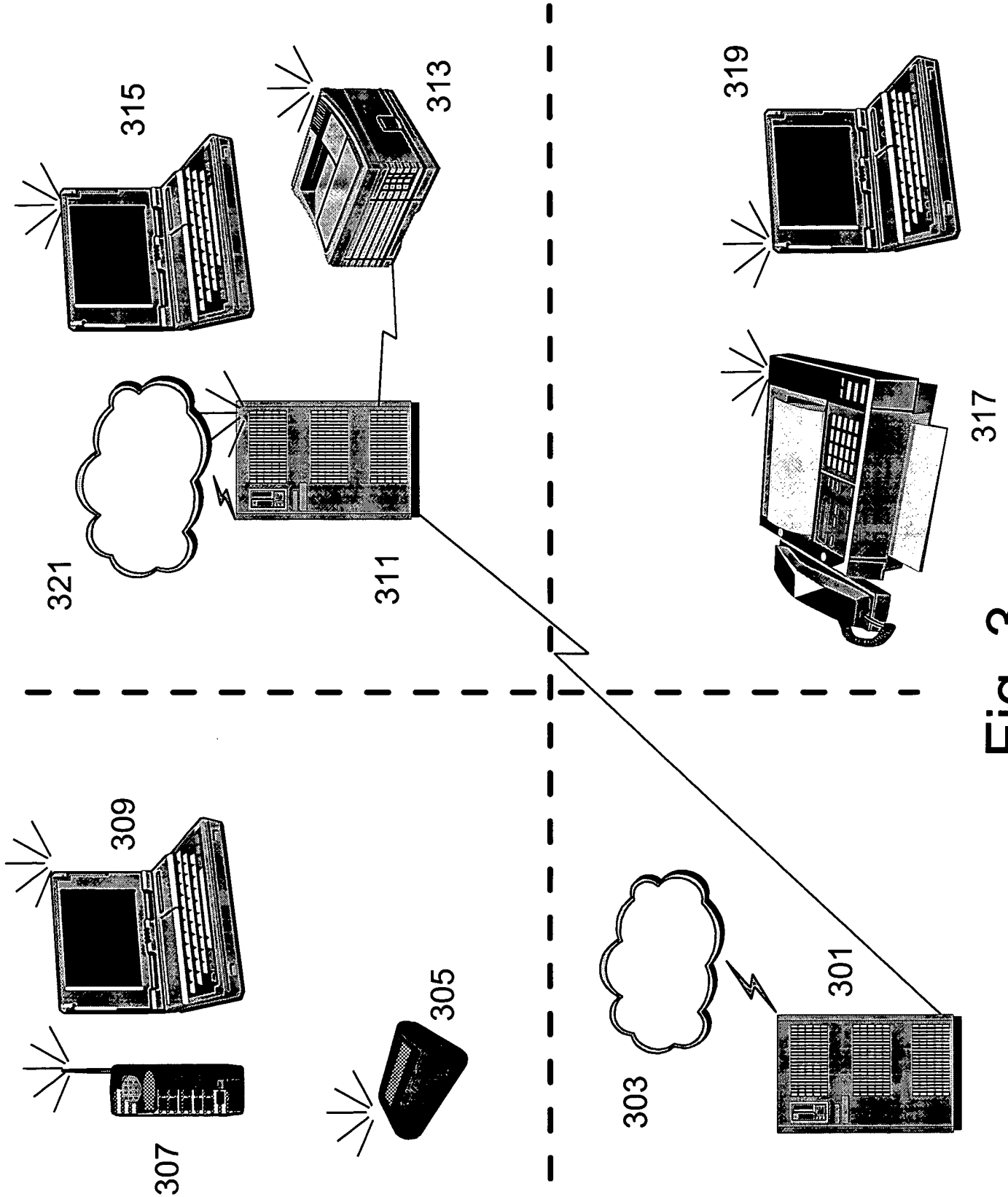


Fig. 3

1050'

| | |
|-------------------|------|
| Device Identifier | 4010 |
| Public Key | 4015 |
| Optional Data | 4020 |

Fig. 4

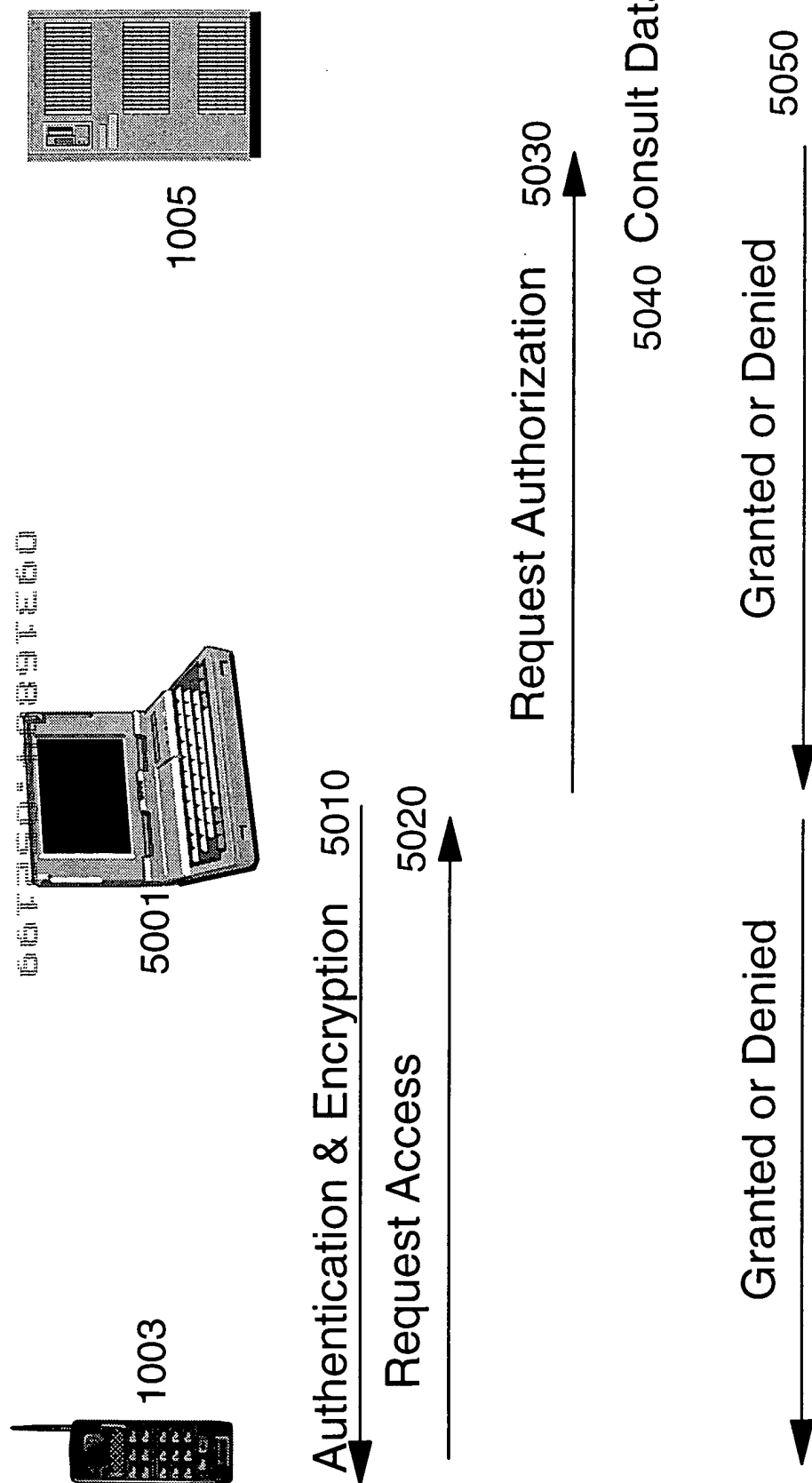
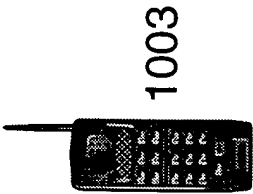
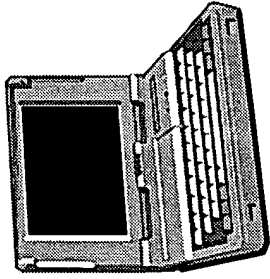


Fig. 5A



66F250-4089F60



1003

5001

Authentication & Encryption

5010

Request Access

5020

5100 Examine Optional
Data in Certificate

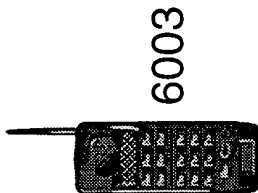
5110 Determine Authorization

Granted or Denied

5150

CA9-99-045
8 of 9

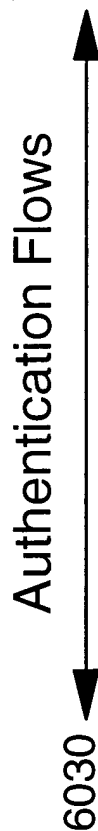
Fig. 5B



Head Set 6001

Unpaired 6010 Unpaired
Device Certificate Present Device Certificate Present

User Initiates Pairing 6020 User Initiates Pairing



6040 Display Device ID from Certificate

User compares device ID displayed with 6050
externally provided device ID

User accepts pairing if they match 6060

User rejects pairing if they don't match 6070

Fig. 6